CNSS Instruction No. 4016
November 2005

National Information Assurance Training Standard For Risk Analysts

Awareness, Training and Education (AT&E) are cost-effective methods of improving organizational Information Assurance (IA). In times of ever-contracting budgets, it is difficult to persuade management to spend money on security and training activities that have no direct impact on the organizational bottom line. This paper describes the proficiencies used to aid in the systematic development of training to serve as the first line of defense in Information Assurance (IA). In addition it describes how these materials are applicable to your organizational long-range plans.

This document provides minimum training standards for those performing risk analyst functions for national security systems. It also may offer guidelines for those performing risk analyst functions for unclassified systems. Your department or agency may require a more stringent implementation.

COMMITTEE ON NATIONAL SECURITY SYSTEMS

CNSSI No. 4016

NATIONAL MANAGER

FOREWORD

1. Since the September 11th terrorist attacks against the sovereignty of the United States and its people, both the President and the Congress have redoubled their efforts to underpin the nation's security. The following guidance, reflecting their support, is intended to assist all federal agencies and private sector concerns in protecting their information systems (ISs). Only through diligence and a well-trained workforce will we be able to defend adequately the nation's vital information resources.

2. This instruction establishes the minimum training standard for the development and implementation of Information Assurance (IA) training for Risk Analysts (RA). The standard presents an in-depth analysis of the range of skills required for persons performing RA functions. RA-related responsibilities may be found throughout government and industry under the guise of other occupational headings such as data analyst, budget analyst, and even to some degree, chief information officer. This standard, while codifying the core performance requirements for a dedicated RA, also provides a set of performance measures which can be incorporated into the definition of positions with RA-related responsibilities in the IA, IT, and management areas.

3. Additional copies of this instruction can be obtained on the CNSS website at www.cnss.gov or by contacting the CNSS Secretariat at the address below.

/s/
KEITH B. ALEXANDER
Lieutenant General, U.S. Army

RISK ANALYST

NATIONAL INFORMATION ASSURANCE (IA)

TRAINING STANDARD FOR RISK ANALYSTS

SECTION I – PURPOSE

1. This instruction establishes the minimum training standard for the development and implementation of Information Assurance (IA) training for Risk Analysts (RA).

SECTION II – REFERENCES

2. Referenced documents are listed in ANNEX B.

SECTION III – DEFINITIONS

3. Definitions in CNSS Instruction No. 4009 (Reference a) and National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501 (Reference b) apply to this instruction.

SECTION IV – APPLICABILITY

4. The President's National Strategy to Secure Cyberspace (Reference c), NSTISSD No. 501, and the Federal Information Security Management Act (FISMA) (Reference d), establish the requirements for federal departments and agencies to implement training programs for IA professionals. An IA professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle. These issuances and others are being implemented in a synergistic environment among departments and agencies committed to satisfying IA education and training requirements. This instruction is a continuation in a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities. (References e through i).

5. ANNEX A lists the minimal IA performance standard for an RA. The body of knowledge listed in this instruction was obtained collaboratively from a variety of sources, *i.e.,* the CNSS Community, industry, and academia.

6. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of IA training for RAs and RA-related positions.

7. Nothing in this policy alters or supersedes the existing authorities of the Director of National Intelligence.

SECTION V – RESPONSIBILITIES

8. Heads of U.S. Government departments and agencies shall ensure that RAs (or their equivalents) are trained to the level of proficiency outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

9. The National Manager shall:

a. Maintain and provide an IA training standard for RAs to U.S. Government departments and agencies.

b. Ensure that appropriate IA training courses for RAs are developed.

c. Assist other U.S. Government departments and agencies in developing and/or conducting IA training activities for RAs as requested.

d. Maintain a national clearinghouse for training and education materials.

Encls:
ANNEX A - Minimal IA Performance Standard for RA
ANNEX B - References

ANNEX A

MINIMAL INFORMATION ASSURANCE (IA) PERFORMANCE STANDARD

FOR RISK ANALYSTS (RA)

FUNCTIONS:

The IA functions performed by personnel engaged in RA activities are:

1. **Information System Life Cycle Activities:** The RA assists other IA professionals in assessing and mitigating risks during the design, development, implementation, operation, maintenance, and disposition phases of information systems life cycle.

2. **Countermeasures Identification, Implementation, and Assessments:** The RA provides a synthesis of risk and countermeasures effectiveness information.

3. **Certification and Accreditation:** The RA provides a repeatable process to assess information system security threats, vulnerabilities and assets and provides risk information to the organization's decision makers.

4. **Synthesis of Analysis:** The RA creates a relevant, sufficient, and comprehensible synthesis of paired-threat/vulnerability, countermeasure, and mission impact information in a context to support decision makers.

5. **Testing and Evaluation:** The RA assesses potential sources of threat that may adversely impact an information system and its associated resources in terms of mission objectives and jeopardy tolerance.

6. **Threat and Adversary Analysis:** The RA assesses potential threats to information systems in terms of mission adversaries, their access to a system, their motivation, and their ability to effect harm.

7. **Mission and Assets Assessments:** The RA assesses how an information system supports a given mission and how a given information system's degradation impacts that mission.

8. **Vulnerabilities and Attack Avenues Analysis:** The RA identifies and characterizes the information system's weaknesses with respect to their cost (resource/jeopardy to themselves) to exploit, an attacker's objectives, access requirements, jeopardy incurred, and the impact on an organization's mission.

9. **Training and Awareness:** The RA serves as a subject matter expert on risk analysis by providing training and informational material to an organization. This material enables trainers to include risk management in courseware and system orientation.

TERMINAL OBJECTIVE:

At the end of training, each skill level will be able to fulfill the following roles:

ENTRY LEVEL: Given various scenarios and typical situations containing information system security issues, the RA under the purview of a more experienced risk analyst will be able to serve as a risk analysis team member, gather information pertinent to IA risk analysis, and provide guidance to IA personnel, *i.e.* system administrators (SAs) and information systems security officers (ISSOs). To be acceptable, the description and application must be in accordance with applicable IA regulations, policies, and guidelines.

INTERMEDIATE LEVEL: Given various scenarios and typical situations containing information system security issues, the RA under the purview of a more experienced risk analyst will be able to interpret and analyze input; explain and recommend appropriate technical, policy, and personnel solutions to system security deficiencies; and to play a leading role in evaluation teams that assess risk. To be acceptable, the description and application must be in accordance with applicable IA regulations, policies, and guidelines.

ADVANCED LEVEL: Given various scenarios and typical situations containing information system security issues, the RA will be able to validate solutions and to verify that the appropriate technical, policy, and personnel remedies to system security deficiencies have been addressed appropriately. The RA also will be able to create new solutions to unexpected problems and to interact with and explain cost/benefit to organizational management. Risk Analysts at the advanced level additionally will be able to mentor and to provide technical guidance to less experienced RAs. To be acceptable, the description and application must be in accordance with applicable IA regulations, policies, and guidelines.

These skill levels* are annotated in the list of performance items under competencies as:

E = Entry Level

I = Intermediate Level

A = Advanced Level

*Note: These levels are linearly hierarchical.

GENERAL BACKGROUND

The following items constitute examples of basic literacies necessary for a Risk Analyst to proceed through the course material based on this standard.

Literacy Necessary for a Risk Analyst at the Entry and Intermediate Level	
Access authorization/permission	Hackers and unauthorized users
Accountability	Information Assurance
Assurance	Information integrity
Audit collection	Intrusion
Automated security tools	Integrity
Business recovery	Life cycle system security
Certification & Accreditation	Penetration testing
Change control policies	Personnel security policies
Classification policies	Physical security
Computer crime	Risk analysis
Configuration management	Risk analysis processes
Continuity of operations	Risk management
Cost benefit analysis	Security laws and regulations
Critical assets	Security policy
Data access control	Security safeguards
Denial of service	Security test and evaluation (ST&E) procedures
Detection and response	Social Engineering
Due diligence	System protection profile
Effect of countermeasures	Threat/vulnerability analyses
Environmental/natural threats	Unauthorized system access
Evidence collections	Vulnerability analysis tools
FISMA	

In each of the competency areas listed below, the RA shall be trained to perform the following functions at the levels indicated:

FUNCTION ONE – INFORMATION SYSTEM LIFE CYCLE ACTIVITIES

Assessing risk throughout system life cycle.

Life Cycle Duties

1. Agency/Vendor Cooperation/Coordination
   I –Analyze roles and responsibilities of agency vendors as members of risk management team
   I – Identify roles and responsibilities of agency vendors as member of risk management team
   A – Recommend changes to roles and responsibilities of agency vendors as member of risk management team

2. System Disposition/Reutilization
   E – Discuss processes for disposition of media and data
   E – Identify agency-specific system reutilization policies and procedures
   I – Examine disposition of media and data records
   A – Analyze disposition and reutilization records for potential vulnerabilities

3. System Configuration and Management Board (SCMB)
   E – Identify life cycle management SCMB policies and procedures
   I – Advise SCMB on risk associated with agency-specific policies and procedures
   I – Apply risk management methodologies to study of life cycle management policies and procedures
   I – Assess the risk of change proposals to authorized baselines
   A – Recommend risk management methodology changes to life cycle management policies and procedures plan

4. Operations & Maintenance (O & M)
   E – Discuss risk analysis processes used in development of life cycle functions
   E – Monitor life cycle operation and maintenance project milestones relating to risk
   E – Monitor maintenance procedures concerning life cycle operations and analysis issues
   E – Monitor performance measurement data in operations and maintenance examination of events and/or changes in an event
   I – Consult records of system activities for chronological, analytical reconstruction,

and maintenance of IA components in IT systems

5. System Acquisition
E – Discuss risk analyst concerns relating to life cycle system security planning
E – Monitor process of selecting and purchasing IT designed to implement management risk process
E – Verify that system acquisitions policies and procedures include assessment of risk management policies
I – Influence process of selecting and purchasing new IT

6. System Administration
E – Discuss audit mechanism processes used to collect, review, and/or examine system activities
I – Recommend software options that control hardware and other software functions
I – Define access permission granted to a subject in relation to an object
I – Define maintenance of user authentication data used to authenticate an identity or to authorize access to data
I – Discuss security software designed to detect and prevent unauthorized system access

7. System Owners
E – Discuss maintenance plans for protective measures to ensure tolerable level of risk
I – Recommend risk management methodologies to evaluate threats, vulnerabilities, and countermeasures to determine residual risk
I – Define legal process for obtaining/maintaining ownership of information

8. System Developers
E – Discuss process for selecting and purchasing new information technology (IT)
E – Discuss process to ensure that applications function according to specifications
E – Explain risk methodologies used to evaluate measures taken to protect system
I – Analyze maintenance practices, procedures, and measures intended to ensure an acceptable level of risk
I - Explain system IA policy with regard to the acquisition and upgrade of software and hardware components and the laws and procedures that must be observed in their implementation

9. Computer Science and Architecture
E – Discuss system IA design guidance
I – Explain collection of verification and validation tools and techniques
I – Explain development of agency-specific IA principles and practices

10. Security Product Integration
E – Examine and analyze applied security

11. Information Systems Security Officer (ISSO) Activities

E – Discuss maintenance of user accounts
E – Discuss processes for timely deletion of accounts
E – Discuss processes for updating access
E – Discuss processes for verification of authorization prior to adding new account
I - Explain system IA policy with regard to the acquisition and upgrade of software and hardware components and the laws and procedures that must be observed in their implementation
I – Discuss maintenance of accounting files, tools, user accounts, and system statistics
I – Explain process used to collect, review, and/or examine system activities

12. Audit Mechanism

E – Review policy, guidance and process for the capture, maintenance, and distribution of audit logs
I – Discuss policies regarding audit data usage, management, and maintenance
I – Discuss policies regarding personnel access to audit records
I – Interpret guidance defining audit collection requirements implementation

13. Policy Development

E – Develop risk management methodology which includes evaluation of threats, vulnerabilities, and countermeasures

14. System Certifiers and Accreditors

E – Explain how certification process ensures security requirement implementation
E – Explain local policies and procedures to supplement and implement higher-level guidance
I – Evaluate operating and management procedures designed to detect or prevent unauthorized access
I – Evaluate operating and management procedures enforcing access control

15. Automated Tool for Security Test

E – Discuss utilities used to determine vulnerabilities or configurations not within established limits/baselines

FUNCTION TWO - COUNTERMEASURES IDENTIFICATION, IMPLEMENTATION, AND ASSESSMENTS

Analyzing countermeasure effectiveness to maximize risk mitigation.

Countermeasures

1. General
   E – Identify all component and overall risks inherent in system
   E – Assist certifier to determine countermeasures based on threat capabilities and motivations
   I – Compare examination and evaluation of potential alternative actions to mitigate risk
   I – Determine effects of risk mitigation derived from system countermeasures
   I – Identify risk variables through compendium of threats, vulnerabilities, attacks and consequences
   I – Recommend specific security and software engineering applications during design, implementation, and testing phases
   A – Analyze paired interaction of defense for specific vulnerability related to probability of attack

2. Analyzing Potential Countermeasures
   E – Discuss security test and evaluation (ST&E) procedures, tools, and equipment
   E – Assist certifier to evaluate security requirements as potential countermeasures
   E – Relate organization IT security needs to countermeasure requirements
   E – Discuss testing roles and responsibilities
   E – Discuss respective value of penetration testing post-testing actions, general information principles, and summary comparison of network testing techniques
   E – Explain process to determine underlying state of system
   I – Apply deductive reasoning to test results
   I – Apply discriminate approach variables and constants based on test procedures to gain acceptance for joint system usage
   I – Assist certifier to determine underlying state of system
   A – Analyze potential applicability of network and vulnerability scanning tools
   A – Analyze potential applicability of range of testing tools
   A – Appraise applicability of network tools, *viz.*, password cracking, log review, file integrity, virus detectors, war dialing, wireless LAN testing (war driving), *etc.* software

3. Determining Countermeasures
   E – Apprise decision makers of existing countermeasure models, tools, and techniques

4. Identifying Potential Countermeasures
   E – Discuss effectiveness of automated security tools that confirm validity of a transmission
   E – Discuss effectiveness of automated security tools that verify an individual's eligibility to receive specific categories of information
   E – Discuss methodologies used to evaluate system security safeguards
   E – Assist certifier/IA engineer to evaluate system security safeguards established to determine system security posture
   I – Research protection profiles for proposed system security countermeasures for a given attack analysis

5. Determining Cost/Benefit of Countermeasures
   E – Outline cost/benefit of organization's IA countermeasure plans
   E – Outline cost/benefit of personnel supporting access control policies
   I – Define cost/benefits of IA plans to determine totality of sensitivity during development, procurement, and installation of system in terms of aggregation of risk
   A – Appraise cost/benefit of standard certification tools to support countermeasure activities

FUNCTION THREE – CERTIFICATION AND ACCREDITATION

Verifying validity of and analyzing results of certification and accreditation (C&A) efforts.

Certification and Accreditation

1. Certification and Accreditation Guidelines and Documentation
   E – Explain applicable organizational certification and accreditation processes
   E – Discuss role of RA in certification and accreditation process
   I – Contrast organizational certification and accreditation process with other agency certification and accreditation guidelines

2. Vulnerabilities and Attacks
   E – Discuss paired interaction of a vulnerability to an attack
   I – Monitor certification/accreditation process for vulnerabilities

3. Approval to Operate
   I – Discuss approval process for operating system at a satisfactory level of risk

4. Security Laws
   E – Outline security laws applicable to certification/accreditation process

5. Physical Security Requirements
   E – Discuss risk mitigation decisions derived from analysis and review of physical security requirements

6. Security Inspections
   E – Evaluate security inspections conducted during C&A process
   E – Discuss security inspections conducted during C&A process
   I – Recommend security inspections during C&A process

7. Security Policies and Procedures
   E – Explain security policies and procedures implemented during risk analysis/assessment process

8. Security Processing Mode
   E – Discuss vulnerabilities associated with security processing modes

9. System Certification
   E – Discuss threat and vulnerability analyses input to C&A process
   I – Define activities that support C&A process

I – Define how C&A provides assurance that controls are functioning effectively

10. Support C&A
E – Identify system security policies
E – Explain alternative actions permitted on system
I – Advise on types and details of actions permitted on systems
I – Assist certifier in analyzing, recommending and detailing alternative actions permitted on system

11. System Security Profile
E – Describe protections offered by security features in specific configurations
E – Discuss security features of system
E – Assist in helping to identify protections offered by security features in specific configurations
I – Provide input for recommending security features in specific configurations

12. Threat/Risk Assessment
E – Identify threat/risk assessment methodology appropriate for use with system undergoing accreditation
A – Perform threat/risk assessment in support of C&A process

13. Information Technology Security Evaluation Criteria
E – Assist in the use of common criteria guidance to determine hardware and software assurance applications for simultaneous processing of a range of information classes

14. Mission
E – Discuss impact of security on mission

15. Interviewing/Interrogation
E – Assist certifier in preparing questions for determining countermeasures during C&A process

16. Applications Security
E – Discuss criticality of applications security

FUNCTION FOUR – SYNTHESIS OF ANALYSIS

Synthesizing the results of IA efforts taken to protect the system and the data processed on it.

Synthesis of Analysis Duties

A. General

1. Synthesis of Components and Overall Risks
   E – Report synthesis of all component and risks inherent in a system

2. Analyze Vulnerabilities and Attacks
   I – Compare analysis of paired interaction of vulnerability to attack

3. Aspects of Security
   E – Discuss security with regard to confidentiality, integrity, authentication, availability, and non-repudiation

4. Assessment Methodology
   E – Appraise information acquisition and review process for best use of resources to protect system

5. Associate Threat Probabilities to Vulnerability
   E – Describe process of analyzing paired interactions of system threats and vulnerabilities

6. Conducting Risk Analysis
   E – Conduct risk analysis examination and evaluation process to determine relationships among threats, vulnerabilities, and countermeasures

7. Countermeasure Analysis
   E – Conduct detailed examination and evaluation of impact of attacks
   E – Conduct detailed examination and evaluation of possible actions to mitigate vulnerabilities

8. Critical Thinking
   E – Discriminate between known and hypothetical variables based on executed test procedures

9. Deductive Reasoning
   E – Analyze tests results

I – Determine underlying state of system

10. Detailed Residual Risk
    E – Discuss susceptibility of a system to attack after countermeasures have been applied
    E – Assist certifier/IA engineer in evaluating susceptibility of a system to attack after countermeasures have been applied

11. Effect of Countermeasures on Risk
    I – Conduct analysis of countermeasure effectiveness as applied to a given risk and probability of an occurrence

12. Effects of Mitigation
    I – Determine effects of mitigation derived from application of countermeasures

13. All Risk Variables
    E – Evaluate an analysis of threats, vulnerabilities, attacks, and consequences in relationship to risk assessment of a system

14. Risk Assessment (Environment & Threat Description)
    E – Discuss environment in relation to current threat

15. Risk Management Methodology
    E – Discuss organizational capability and ability to evaluate threats, and vulnerabilities

16. Security Countermeasures
    E – Assist certifier/IA engineer in defining countermeasures directed at specific threats and vulnerabilities

17. Technical Vulnerability
    E – Discuss hardware, firmware, communications, or software weaknesses that open an information system to exploitation

18. Threat Analysis
    E – Examine methods through which threat agent adversely affects information system, facility, or operation

19. Threat Description
    E – Define means through which a threat agent can adversely affect information system, facility, or operation

20. Threat/Risk Assessment

E – Discuss process of formally evaluating degree of threat and describing nature of threat

21. Mission
    E – Discuss information system support mission
    I – Determine offsets of adverse findings and decision to continue IT operation in current mission environment

22. Vulnerabilities
    E – Assist in identifying weakness in an information system, system security procedures, internal controls, or implementation that could be exploited
    E – Discuss weakness in an information system, system security procedures, internal controls, or implementation that could be exploited
    E – Explain hardware or software flow that opens an information system to potential exploitation

23. Vulnerability Analysis
    E – Analyze an information system to determine adequacy of security measures
    I – Analyze weakness in an information system, system security procedures, internal controls, or implementation that could be exploited
    I – Identify security deficiencies
    I – Assist certifier/IA engineer provide data that confirms effectiveness of security measures after security testing
    I – Assist certifier/IA engineer to provide data to predict effectiveness of a security measure testing

B. Documentation

1. Policies
   I – Identify applicable national level and agency/local policies and guidance
   E – Explain applicable national level policies
   E – Discuss agency/local guidance

2. Access Control Policies

I - Explain system IA policy with regard to the acquisition and upgrade of software and hardware components and the laws and procedures that must be observed in their implementation

3. Formal Methods for Security Design
   I – Team with certifier/IA engineer to evaluate collection of languages and tools that enforce methods of verification

4. Generally Accepted Systems Security Principles

I – Team with certifier/IA engineer to evaluate acceptability of using federal information security practices in system design and protection
A – Team with certifier/IA engineer to plan and coordinate development of IA principles and practices applied to coordination with OMB and with technical assistance from NSA

5. Information Security Policy
I – Evaluate security policies that describe permitted actions that may have an adverse affect on system

6. Laws, Regulations, and Other Public Policy
I – Evaluate the implementation of laws, regulations and other public policies as they apply to an information system in a given operational environment

7. Life Cycle System Security Planning
A – Team with certifier/IA engineer to evaluate integrated logistics support cycle as it applies to IA

8. Personnel Security Policies and Guidance
I – Team with certifier/IA engineer to evaluate the implementation of established policies and procedures ensuring that personnel have required authority and appropriate clearances

9. Technical Knowledge of Information System
E – Outline technical knowledge required of personnel responsible for networks, servers, workstations, operating systems, *etc.*

10. Threat/Risk Assessment
A – Evaluate process of evaluating degree of threat to an information system
A – Evaluate process of evaluating nature of threat to an information system

11. Mission
I – Evaluate current mission and determine if an adverse system finding should be allowed to halt mission support operations

C. Effect of Countermeasure

1. Access Control Policies
I – Team with certifier/IA engineer to evaluate operating and management procedures designed to detect or prevent unauthorized access to an information system
I - Explain system IA policy with regard to the acquisition and upgrade of software and hardware components and the laws and procedures that must be observed in their implementation

2. Agency-Specific Policies and Procedures
   I – Team with certifier/IA engineer to evaluate local policies and procedures that implement higher-level regulations, laws, and procedures

3. Cost/Benefit Analysis
   I – Evaluate assessment of data protection costs versus loss or compromise of data

4. Countermeasures
   I – Discuss actions, devices, procedures, techniques, or measures that reduce vulnerability or threat to a system

5. Life Cycle System Security Planning
   I – Evaluate allowable duration of system's operations run time, beginning with identification of a need to place a system in operation; continuing through system design, development, implementation, and operation; and ending with the system's deactivation and disposal

6. Network Firewalls
   I – Team with certifier/IA engineer to evaluate protection afforded information processed in a cryptographically-secured network

7. Preventative Controls
   I – Team with certifier/IA engineer to check accuracy and reliability of an information system's data
   I – Team with certifier/IA engineer to evaluate controls to safeguard assets
   I – Team with certifier/IA engineer to promote an information system's operational efficiency
   I – Team with certifier/IA engineer to encourage adherence to prescribed managerial policies

8. Security Domains
   I – Explain how physical security and domains provide a useful approach for dealing with security and data protection in large-scale systems
   I – Team with certifier/IA engineer to evaluate how physical security and domains provide a useful approach for dealing with security and data protection in large-scale systems

9. Security Product Testing/Evaluation
   E – Examine analysis of security safeguards of a system as they have been applied to an operational environment to determine security posture

10. Technical Knowledge of Information System
    E – Outline technical knowledge required of personnel responsible for operating and

maintaining networks, servers, workstations, operating systems, *etc.*

11. Technological Threats
    I – Evaluate hardware, software, firmware, communication flaw, circumstance, or event with potential to cause harm to a system or data

12. Threat/Risk Assessment
    I – Evaluate life cycle analysis of security requirements and countermeasures based on assessment of threats capability and motivation to exploit a vulnerability

13. Mission
    A – Evaluate affects of a risk assessment and certification/accreditation process on mission of a system

FUNCTION FIVE – TESTING AND EVALUATION

Working with other IA professionals to evaluate risk mitigation through testing and evaluation.

Testing and Evaluation Duties

1. Access Authorization
   I – Team with certifier/IA engineer to evaluate formal approval process and procedures for providing system access for authorized users

2. Access Privileges
   I – Team with certifier/IA engineer to evaluate access permissions granted to users of system

3. Account Administration
   E – Discuss maintenance of accounting files, tools, user accounts, and system statistics

4. Assessment Methodology
   E – Define vulnerability analysis process

5. Associate Threat Probabilities to Vulnerability
   E – Explain paired interaction of system threats and vulnerabilities

6. Audit Trails and Logging
   E – Team with certifier/IA engineer to compile chronological record of system activities for reconstruction and examination of events and/or changes in an event

7. Backups
   E – Discuss purpose of using copies of backup files for later reconstruction of files

8. Software Test & Evaluation Results
   E – Ensure software test and evaluation results related to system restoration are performed

9. Certification
   I – Assist with evaluation of technical and non-technical security features of system during testing and evaluation

10. Change Controls
    I – Team with certifier/IA engineer to evaluate controls and traceability for all changes made to system during testing and evaluation

11. <u>Client/Server Security</u>
    I – Team with certifier/IA engineer to evaluate protection schema of a distributed system that consists of workstations

12. <u>Security Test & Evaluation Plan & Procedure</u>
    E – Assist with the development of ST&E plan and procedure for testing and evaluating a system

13. <u>Error Logs</u>
    E – Interpret files created by operating system for review of audit process

14. <u>Non-Technical & Technical Result</u>
    E – Interpret technical and non-technical results from testing and evaluation

15. <u>Evaluation Techniques</u>
    E – Team with certifier/IA engineer to integrate technical analysis of components, products, subsystems, or systems security that establishes whether or not component, product subsystem, or system meets a specific set of requirements independently and in collaborative operations

16. <u>Identify All Risk Variables</u>
    E – Explain development of a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system (Common vulnerabilities and exploitations)

17. <u>Identify Potential Corrective Approaches</u>
    I – Team with certifier/IA engineer to generate database of corrective measures to bring system into compliance of level for which being certified

18. <u>Certification Tools</u>
    E – Team with certifier/IA engineer to interpret results of certification tools during testing and evaluation

19. <u>Privileges (Class, Nodes)</u>
    E – Influence program or user operations that can be performed during testing and Evaluation

20. <u>Test and Evaluation Strategies</u>
    E– Identify strengths of alternative test and evaluation strategies
    I – Evaluate the relative strengths of alternative test and evaluation strategies

21. Testing Implementation of Security Features
    E – Integrate testing of security features during testing and evaluation

FUNCTION SIX – THREAT AND ADVERSARY ANALYSIS

Analyzing the nature and degree of system risks.

Threat and Adversary Analysis Duties

A. General

1. Conducting Risk Analysis
   E – Conduct examination of vulnerabilities, attack, threats and consequences that may affect system

2. Cost/Benefit Analysis
   E – Conduct an assessment of costs of data protection for a system versus cost of loss or compromise

3. Critical Thinking
   E – Discuss known and hypothetical variables based on test procedures

4. Deductive Reasoning
   E – Recommend solutions based on a set of static and variable factors of system

5. Effects of Mitigation
   E – Determine effects of mitigation derived from application of countermeasures to a system

6. Hostile Intelligence Sources
   E – Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security

7. All Risk Variables
   E – Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system

B. Risk Assessment (Environment & Threat Description)

1. Risk Management Methodology
   E – Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk

2. Security Countermeasures

E – Discuss security and software countermeasures during design, implementation, and testing phases to achieve required level of confidence

3. Threat Analysis
E – Conduct examination and evaluation of sources and factors that can adversely impact system

4. Treat Description
E – Identify level of threat based on its applicability to system

5. Threat/Risk Assessment
E – Recommend life cycle countermeasures based on assessments of threats, capabilities, and motivations to exploit vulnerability

6. Mission
E – Discuss current mission and role of information system in supporting mission
E – Determine if an adverse system finding should be allowed to halt mission support operations

7. Vulnerability Analysis
E – Appraise weaknesses in information system, security procedures, internal controls, or implementations that could be exploited

C. Analysis for Decisions

Analysis for Decisions
A – Team with certifier/IA engineer to determine countermeasures
A – Interpret system vulnerabilities

D. Agency-Specific Policies and Procedures

Agency-Specific Policies and Procedures
E – Discuss local policies and procedures implementing regulations, laws, and procedures in local environment

E. Assessment Methodology

Assessment Methodology
I – Team with certifier/IA engineer to determine method used for surveys and inspections in C&A process
I – Discuss analysis of vulnerabilities of an information system

F. Audit Trails and Logging Policies

Audit Trails and Logging Policies
I – Discuss policies regarding audit data usage, management, and maintenance
I – Discuss policies regarding personnel access to audit records
I – Team with certifier to interpret guidance defining how audit collection requirements are to be implemented

G. Information Integrity

Information Integrity
I – Discuss characteristics that ensure computer resources operate correctly
I – Discuss characteristics that ensure data integrity
I – Discuss security policies that describe permitted system actions
I – Discuss security policies that describe what system actions are prohibited

H. Technical Surveillance Countermeasures

Technical Surveillance Countermeasures
E – Discuss Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies

FUNCTION SEVEN – MISSION AND ASSETS ASSESSMENTS

Determining role and criticality of information systems in supporting organizational mission.

Mission and Assets Duties

A. General

1. Conducting Risk Analysis
   E– Conduct detailed evaluation of vulnerabilities, attack, threats, and consequences that may affect system
   E– Conduct detailed examination of vulnerabilities, attack, threats, and consequences that may affect system

2. Cost/Benefit Analysis
   E – Conduct cost assessment for providing data protection versus cost of data loss or compromise

3. Critical Thinking
   E – Understand known and hypothetical variables based on test procedures

4. Deductive Reasoning
   E – Recommend solutions based on a set of static and variable factors

5. Effects of Mitigation
   E – Determine effects of mitigation derived from application of countermeasures

6. Hostile Intelligence Sources
   E – Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security

7. All Risk Variables
   E – Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system

B. Risk Assessment (Environment & Threat Description)

1. Risk Management Methodology
   E – Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk

2. Security Countermeasures
   E – Discuss security and software countermeasures during design, implementation and testing phases to achieve required level of confidence

3. Threat Analysis
   E – Conduct detailed examination and evaluation of sources and factors that can adversely impact system
   I – Incorporate relevant potential threat/vulnerability information gained from available intelligence and law enforcement agency sources

4. Treat Description
   E – Identify level of threat based on its applicability to system

5. Threat/Risk Assessment
   E – Recommend life cycle countermeasures based on assessment of threats, capabilities, and motivations to exploit vulnerability

6. Mission
   E – Assess mission to determine if an adverse finding should be allowed to affect continued IT operations in a given mission environment

7. Vulnerability Analysis
   E – Appraise exploitable weaknesses in information system, security procedures, internal controls or implementations

C. Analysis for Decisions

Analysis for Decisions
A – Interpret system vulnerabilities
A – Determines countermeasures

D. Agency-Specific Policies and Procedures

Agency-Specific Policies and Procedures
E – Discuss local policies and procedures implementing regulations, laws, and procedures in local environment

E. Assessment Methodology

Assessment Methodology

I – Determine method used for surveys and inspections in C&A process
I – Discuss analysis of vulnerabilities of an information system

F. Audit Trails and Logging Policies

Audit Trails and Logging Policies
I – Discuss policies regarding audit data usage, management, and maintenance
I – Discuss policies regarding personnel access to audit records
I – Interpret guidance defining how audit collection requirements are to be implemented

G. Information Integrity

Information Integrity
I – Define security processes that ensure computer resources operate correctly and that data in databases are correct
I – Discuss security policy that describes types of permitted and prohibited actions on system

H. Technical Surveillance Countermeasures

Technical Surveillance Countermeasures
E – Discuss techniques and measures to detect and neutralize hostile penetration technologies

FUNCTION EIGHT – VULNERABILITIES AND ATTACK AVENUES ANALYSIS

Evaluating system weaknesses and adversary techniques.

Vulnerability and Attack Avenues Duties

A. General

1. Vulnerabilities, attacks, threats, and consequences
   E – Assess vulnerabilities, attacks, threats, and consequences to determine vulnerabilities and attack avenues

2. Cost/Benefit Analysis
   E – Discuss cost analysis of data protection versus cost of data lose or compromise

3. Critical Thinking
   E – Apply discrimination to known and potential vulnerabilities based on test procedures

4. Deductive Reasoning
   E – Use test results to determine underlying state of system

5. Effect of Countermeasures on Risk
   E – Determine effect of countermeasures on risk through the analysis of paired interaction of a defense

6. Effects of Mitigation
   E – Determine effects of mitigation derived from application of countermeasures to system

7. Hostile Intelligence Sources
   E – Discuss hostile intelligence sources as part of vulnerabilities and attack venues

8. Risk Variables
   E – Identify risk variables to build a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system

9. Jamming
   E – Discuss jamming as a potential threat

10. Risk Assessment
    E – Define risk assessment methodology in relation to risk analyst function

11. Risk Management Methodology
    E – Define risk management methodology in relation to system security

12. Security Countermeasures
    E – Discuss security countermeasures in relation to vulnerabilities and attack venues

13. Threat Analysis
    E – Use threat analysis to determine vulnerabilities and attack venues

14. Threat/Risk Assessment
    E – Apply threat and/or risk assessment in determining vulnerabilities and attack venues

15. Mission
    E – Support organizational mission in conjunction with vulnerabilities and attack venues

16. Vulnerabilities
    E – Discuss weaknesses in system, system security procedures, and internal controls and implementation

17. Vulnerability Analysis
    E – Use vulnerability analysis to determine adequacy of security measures, identify security deficiencies, and provide data to predict effectiveness of security measures

B. Developing Attack Avenues

Avenues of Attack
E – Describe known avenues of attack such as operating system bugs, network vulnerabilities, human threats, *etc*.

C. Characterizing Vulnerabilities

Characterizing Vulnerabilities
E – Discuss aspects of security in a vulnerability testing and evaluation plan
E –Evaluate threats and vulnerabilities

D. Researching Vulnerability Report

Researching Vulnerability Report
E –Evaluate vulnerability assessment methodologies

E. Collecting and Reviewing Vulnerabilities

Collecting and Reviewing Vulnerabilities
E – List potential vulnerabilities that may lead to defeat of security services
I – Incorporate relevant potential vulnerability/threat information gained from intelligence and law enforcement agency sources

F. Comparing and Contrasting Attack Avenues

Comparing and Contrasting Attack Avenues
E – Discuss techniques and measures to detect or neutralize a wide variety of hostile penetration technologies
E – Evaluate payoff to and liabilities incurred by an attacker in a successful attack
I – Justify technical surveillance countermeasures

G. Risk of Detection and Response

Risk of Detection and Response
E – Characterize impact of security breaches and estimate an attacker's probable Response

H. Cost of Attack

Cost of Attack
I – Discuss return on investment results of evaluation of means by which threats can act on vulnerabilities
I – Discuss aspects of security for a system and cost incurred by an adversary to mount an attack

I. Technology Necessary to Mount Attack

Technology Necessary to Mount Attack
E – Describe technology needed to mount an attack based on existing countermeasures

FUNCTION NINE – TRAINING AND AWARENESS

Sharing IA analytical expertise and lessons learned from other IA professionals, prepare both on-line and stand-up training and awareness products.

Training and Awareness Duties

A. Policies/Procedures/Methodology

1. Access Control Policies
E – Summarize national and local level access control policies
I – Recommend implementation policies
I – Demonstrate effect of modification to existing access controls
A – Define system level access policies used to process information

2. Laws, Regulations, and Other Public Policy
E – Identify local application of IA laws, regulations, and policies
E – Discuss applicable IA laws, regulations, and policies
A – Explain application of IA laws, regulations, and policies

3. Agency-Specific IA and IT Policies and Procedures
E – Summarize agency-specific policies and procedures in relation to risk environment
I – Discuss agency-specific policies and procedures
I – Integrate agency-specific policies and procedures into results of risk analysis report

4. Assessment Methodology
I – Assist in integration of a variety of assessment methodologies into curricula
A – Provide interpretation of strengths and weaknesses of assessment methodologies

5. Audit Trails and Logging Policies
E – Discuss audit trails and logging policies
I – Provide audit trail and logging policy examples for training
I – Explain role of audit trails

6. Change Control Policies
E – Discuss change control policies for incorporation in IA training
I – Explain change control policies for incorporation in IA training
I – Influence change control policies in corporation in IA training

7. Communications Security Policy and Guidance
A – Interpret communications security policy and guidance for incorporation into IT

training
E – Discuss communications security policy and guidance for incorporation into IT training
E – Identify communications security policy and guidance for incorporation into IT training
I – Explain communications security policy and guidance for incorporation into IT training

8. Emergency Destruction Planning and Procedures (EDPP)
E – Discuss EDPP for incorporation in IA training
I – Explain EDPP for incorporation in IA training

9. Personnel Security Policies and Guidance
E – Discuss role of personnel security policies and guidance as part of overall risk management plan

10. Formal Methods for Security Design
E – Outline role of formal methods in security design as part of risk management plan

11. Information Categorization
E – Discuss various categorization schemas
I – Explain role of information categorization schema as part of risk management plan

12. Information Classification
E – Discuss classification policies as part of risk management plan
I – Explain classification policies as part of risk management plan

13. Knowledge and/or Awareness of Security Laws
I – Outline security laws and applicability to risk management plan

14. Methods of Defining Security Requirements
E – Discuss definitions of security requirements
I – Compare and contrast various methods for defining security requirements

15. Physical Security Requirements
E – Discuss physical security requirements
I – Summarize physical security requirements

16. Risk Acceptance Process
I – Explain risk acceptance process to include mitigation versus avoidance

17. Risk Management Methodology
E – Summarize approaches to risk management

18. Security Awareness
I – Explain role of security awareness as part of risk management plan

19. Ethics
I – Give examples of lessons learned in ethical/unethical cyber behavior and relate to risk management plan

B. Technology

1. Applications Security
E – Discuss state of security features embedded in commercial-off-the-shelf (COTS) products in relation to risk management plan

2. Database Security Features
E – Discuss elements of database security features
E – Identify critical database security pitfalls
E – List database best practices and pitfalls in database security

3. Distributed Systems Security
E – Discuss risks associated with distributed systems security

4. Firmware Security
E – Discuss differences between security features and capabilities

5. Industrial Security
I – Explain rules and measures in place for implementing IA measures with industrial partners/contractors

6 Multi-Discipline Security
I – List relations between variety of disciplines employed in IA
I – Explain relations between variety of disciplines employed in IA

7. Network Security Software
E – Discuss state and vulnerabilities in network security software

8. Remanence
I – Explain threats and vulnerabilities associated with remanence

9. Technology Trends
   E – Summarize technology trends in context of future security management plan

10. Environmental/Natural Threats
    E – List environmental and natural threats as part of security management plan
    E – Discuss environmental and natural threats as part of security management plan

ANNEX B

REFERENCES

a. CNSS Instruction No. 4009, "National Informational Assurance (IA) Glossary," dated 19 May 2003.

b. NSTISS Directive No. 501, "National Training Program for Information Systems Security (INFOSEC) Professionals," dated 16 November 1992.

c. "The National Strategy to Secure Cyberspace, Priority III: A National Cyberspace Security Awareness and Training Program," dated February 2003.

d. "Federal Information Security Management Act of 2002 (FISMA)," contained under Title III of the "Electronic Government Act," dated December 17, 2002.

e. NSTISS Instruction No. 4011, "National Training Standard for Information Systems Security (INFOSEC) Professionals," dated 20 June 1994.

f. NSTISS Instruction No. 4015, "National Training Standard for Systems Certifiers," dated December 2000.

g. CNSS Instruction No. 4012, "National Information Assurance Training Standard for Senior System Managers, dated June 2004.

h. CNSS Instruction No. 4103, " National Information Assurance Training Standard for System Administrators (SA)," dated March 2004.

i. CNSS Instruction No. 4014, "National Information Assurance Training Standard for Information Systems Security Officers," dated April 2004.